스마트 홈 환경에서 IoT 장치의 보안 강화를 위한 Hyperledger Fabric 기반 Architecture

박지호*, 맹주현*, 조인휘*
*한양대학교 컴퓨터 소프트웨어학과
rotc5697@hanyang.ac.kr, jhmaeng@hanyang.ac.kr, iwjoe@hanyang.ac.kr

Hyperledger Fabric Based Architecture for Enhanced Security of IoT Devices in Smart Home Environments

Ji-Ho Park*, Ju-Hyun Maeng*, In-Whee Joe*
*Dept. of Computer Software, Han-Yang University

요 약

최근, 다양한 정보의 수집 및 처리가 필요한 스마트 홈, 의료, 교통, 제조 등 여러 산업 분야에서 IoT(Internet of Things)가 많이 활용되고 있다. 특히 스마트 홈 환경에서 IoT 장치로 수집되는 정보는 민감한 개인 정보를 포함할 수 있기 때문에 특정 그룹이나 개인만이 해당 정보에 접근할 수 있도록 관리할 필요가 있다. 또한, IoT 환경에서 Blockchain 기반으로 데이터의 신뢰성을 확보하는 분산 저장소의 경우, 지연 시간의 증가 문제가 발생될 수 있기 때문에 실시간 데이터 수집에 대한 처리 속도를 향상할 방안이 필요하다. 본 논문에서는 사용자와 IoT 장치 간 생성한 그룹 ID 로 해당 그룹에 대한 접근 권한을 관리하고, Hyperledger Fabric 과 별도의 데이터베이스 운용으로 실시간성, 신뢰성을 향상할 수 있는 Hyperledger Fabric 기반 스마트 홈 Architecture 를 제안한다. 이 Architecture 는 IoT 장치가 사용되는 다양한 환경에서 보안성, 실시간성, 신뢰성을 향상할 수 있을 것이다.

1. 서론

기존 IoT(Internet of Things)의 사람과 사람 사이 통신이라는 개념은 음성에서 정보로, 그 정보가 장치에서 사람 및 사물(Things)이라는 개념으로 확장되었다. [1] 지속적으로 IoT 의 시장 규모가 커지고, 발전하면서 다양한 IoT 장치가 등장하였다. 그러면서 여러 산업 분야에서 IoT 가 활용되고 있다. 이처럼 IoT 의 활용도가 높아지면서 다양한 정보들이 공유되다 보니 특정 그룹 또는 개인만이 해당 정보에 접근하도록 관리하는 구조에 대한 필요성이 대두되었다. 최근 Privacy 침해 사건으로 IP Camera 의 정보를 탈취하여 개인의 사생활을 불법 촬영하고 유포하는 사건이 발생하기도 하였다. 기존 PC 환경에서는 이와 같은 보안 이슈를 개선하기 위한 해결책으로 활용되는 수많은 보안 솔루션이 존재한다. 하지만 IoT 장치의 전력 공급 문제와 연산 능력에 한계 때문에 적용이 쉽지 않다. 그리고 기존 IoT 환경에서 Blockchain 기반으로 데이터의 무결성을 보장하면서 안전하게 데이터를 공유하는 분산 저장소에 대한 연구가 많이 진행되고 있다. 하지만 실시간으로 다양한 정보를 수집하는 IoT 장치의 경우, Blockchain 기반으로 데이터 저장소를 구축하면 처리에 대한 지연시간의 증가 문제가 발생될 수 있다. 본 논문에서는 Hyperledger Fabric 기반 스마트 홈 시스템을 구성하여서 특정 그룹 또는 개인만이 해당 데이터에 접근할 수 있도록 하면서, 별도 데이터베이스의 운용으로 보안성과 실시간성 그리고 신뢰성을 향상하는 방안을 제안한다. 논문의 구성은 다음과 같다. 먼저 2 장에서는 관련 연구를 소개하고, 3 장에서 Hyperledger Fabric 기반 스마트 홈 시스템을 제안한다. 4 장에서는 기대효과를 설명한 후, 마지막으로 5 장에서 결론을 맺는다.

2. 관련 연구

2.1 Hash

Hash 함수는 임의 길이의 입력값을 고정 길이의 출력값으로 변환하는 함수이다. Hash 함수의 출력값은 해시 섬, 해시 체크 섬, 해시 코드로 불리기도 하지만, 간단하게 Hash 라 불린다. Hash 함수는 암호학적 해시

함수와 비 암호학적 해시 함수로 구분된다. 암호학적 해시 함수는 세 가지 특성을 만족해야만 한다. 세 가지 특성으로는 첫 번째는 Hash 출력값의 복호화가 어렵다는 제 1 역상 저항성, 두 번째는 입력값이 같으면 출력값의 변경이 어렵다는 제 2 역상 저항성, 마지막으로 세 번째는 같은 Hash 출력값을 갖는 두 개의 입력값을 찾는 것이 어렵다는 충돌 저항성이다. 이러한 특성을 기반으로 하여서 여러 보안 분야에서 활용되고 있다.

2.2 Blockchain

Blockchain 은 분산 원장 기술이라고도 불리며, 거래 정보를 기록한 원장을 특정 기관의 중앙 서버가 아닌 Peer-to-Peer 네트워크에 분산 저장하여서 참여자가 데이터를 공동으로 기록하고, 관리하는 기술이다. 특히 저장된 데이터의 조작이 어렵다는 특징을 가지고 있다. 대표적 가상 화폐인 Bitcoin 은 Blockchain 기반 기술이다. Blockchain 은 크게 Public Blockchain 과 Private Blockchain 구조로 나뉠 수 있다. 대표적인 Public Blockchain 은 Bitcoin 과 Ethereum 이며, Hyperledger Fabric 은 Private Blockchain 이다.

2.3 Hyperledger Fabric

Hyperledger Project 는 2015 년 Linux 재단과 IBM 의 주도로 시작되었다. Hyperledger Fabric 은 IBM 에서 만든 모듈형 Architecture 기반의 오픈소스 Blockchain Framework 이다. [2]

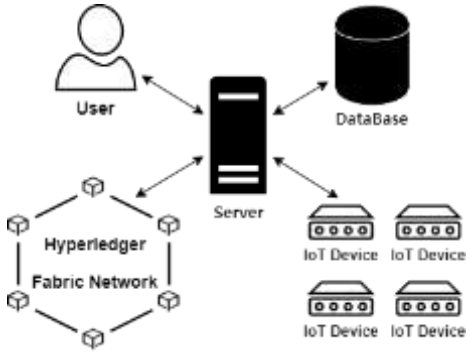
<표 1> Blockchain 비교

구분	Bitcoin	Ethereum	Hyperledger Fabric
유형	비 허가형	비 허가형	허가형
프로그램	없음	Smart Contract	chain Code
내부 통화	있음	있음	없음
거래 수수료	있음	있음	없음
거래 처리방식	순차적	순차적	병렬적
합의 알고리즘	작업 증명	작업 증명	비 작업 증명
속도	약 7 TPS	약 23 TPS	약 1000 TPS
멀티 블록체인	미 지원	미 지원	지원

표 1 과 같이 Hyperledger Fabric 은 허가받은 사용자만이 Network 에 참여 가능하며, 멀티 블록체인을 통한 기밀 유지로 보안성을 강화하였다. 그리고 Membership, Chaincode, Blockchain 으로 구성되고, Endorser, Orderer, Membership, Committer 가 상호작용하면서 Client 의 요청을 처리한다. [3]

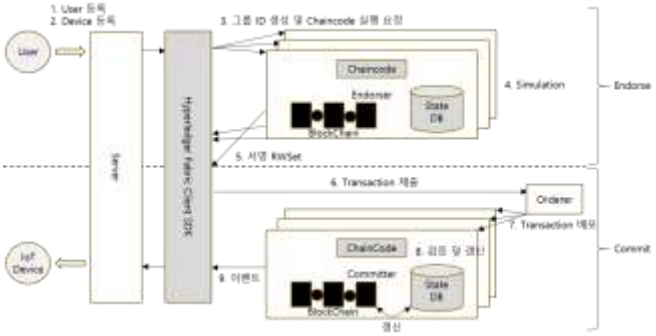
3. 본론

제안하는 시스템은 그림 1 과 같이 Hyperledger Fabric, 서버, 사용자 데이터베이스, IoT 장치로 구성된다.



(그림 1) 제안하는 시스템의 구성

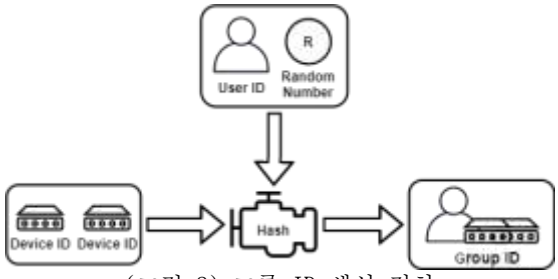
시스템에서는 악의적 사용자가 특정 IoT 장치에 접근하는 것을 차단하기 위하여 먼저 사용자와 IoT 장치 사이의 그룹 ID 를 생성하고, 이 ID 로 그룹을 구성한다. 그리고 Hyperledger Fabric 에서 IoT 장치로부터 수집되는 데이터를 처리하는 것은 지연시간의 증가 문제가 발생될 수 있기 때문에 별도 데이터베이스를 통하여 해당 데이터를 처리한다. Hyperledger Fabric 은 IoT 장치 및 사용자 정보, Transaction(데이터 수집 시간, 장치 제어 이력, 수집 데이터에 대한 해시 등)을 저장하며, 서버는 IoT 장치와 사용자, Hyperledger Fabric, 데이터베이스 사이를 중개한다. 데이터베이스는 IoT 장치로부터 수집되는 데이터를 저장하고, IoT 장치는 데이터를 제공하며, 사용자는 수집된 데이터의 조회와 IoT 장치에 대한 제어 요청을 한다. [4]



(그림 2) 사용자 및 IoT 장치의 등록 절차

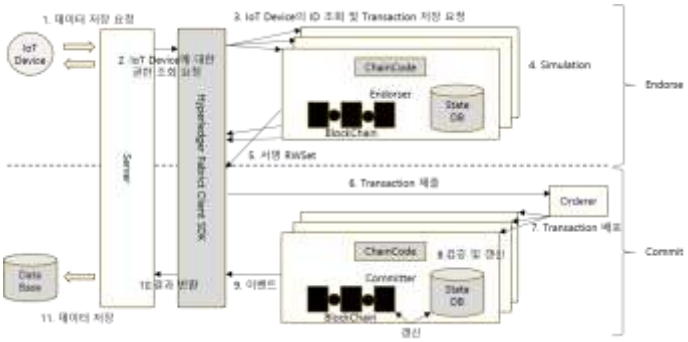
사용자 및 IoT 장치의 등록 절차는 다음과 같다. 먼저 사용자는 인증 서버를 통하여 등록 및 IoT 장치

에 대한 등록 요청을 한다. 서버는 요청에 따라서 그룹 ID 를 생성하고, Hyperledger Fabric 에 이를 저장한다. IoT 장치와 사용자는 서버를 통하여 인증한 후, 데이터 전송을 한다.



(그림 3) 그룹 ID 생성 절차

그림 3 과 같이 사용자 ID 및 등록된 사용자가 관리하는 IoT 장치의 ID, 사용자의 회원 가입 시 생성된 무작위 난수로 그룹 ID 가 생성된다. [5]



(그림 4) 수집 데이터의 저장 절차

IoT 장치로부터 수집되는 데이터의 저장 절차는 다음과 같다. 먼저 IoT 장치는 서버에 데이터의 저장 요청을 하고, 서버는 Hyperledger Fabric 에 IoT 장치에 대한 접근 권한을 확인한 후, Transaction 생성 요청을 한다. Hyperledger Fabric 은 IoT 장치에 대한 권한 확인 후, Transaction 을 저장하고, 서버에 결과를 반환한다. 서버는 반환된 결과를 확인한 후, 데이터베이스에 수집된 데이터에 대한 저장 요청을 하며, 데이터베이스는 요청에 따라서 데이터를 저장한다.

4. 기대 효과

4.1 보안성 향상

그룹 ID 로 사용자와 IoT 장치를 관리하는 구조를 통하여 악의적 사용자가 해당 IoT 장치에 대한 정보를 탈취하더라도 장치로의 접근을 차단할 수 있기 때문에 보안성 향상이 기대된다.

4.2 실시간성 향상

IoT 장치 정보, 사용자 정보, IoT 장치의 수집 이력, 수집 데이터에 대한 해시 값 등의 정적인 데이터만을 Hyperledger Fabric 에 저장하는 구조를 통하여 IoT 장치로부터 수집되는 데이터 처리에 대한 실시간성 향상이 기대된다.

4.3 신뢰성 확보

Hyperledger Fabric 에 저장된 수집 데이터의 해시값과 데이터베이스에 저장된 데이터의 해시값을 비교하는 구조를 통하여 데이터의 위· 변조를 확인하기 때문에 수집되는 데이터의 신뢰성 향상이 기대된다.

5. 결론

스마트 홈 환경에서는 민감한 개인 정보에 대한 접근 관리와 데이터의 신뢰성을 확보하는 분산 저장소에서의 데이터 처리 속도를 향상할 방안이 필요하다. 그래서 우리는 사용자와 IoT 장치 사이의 그룹 ID 를 생성하고, 이 ID 로 장치에 대한 접근 권한을 관리하며, Hyperledger Fabric 과 별도 데이터베이스를 운용하는 구조를 통하여 보안성, 실시간성, 신뢰성을 향상할 수 있는 스마트 홈 시스템을 제안하였다. 추후, 제안한 Architecture 의 성능과 효용성 평가를 진행할 것이다.

참고 문헌

[1] 김영로, "사물인터넷이 세상을 바꾼다" SW 중심사회, 2016

[2] https://hyperledger-fabric.readthedocs.io

[3] 김주성, 조인휘, 맹주현, 미래戰에 대비한 국방 무기・정보체계 블록체인기술 융합 방안 국방과 보안, 제 1 권 제 2 호, pp. 92- 117, 2019

[4] 박태준, 블록체인과 IoT 네트워크 기술, 정보과학회지 제 36 권 제 5 호, pp. 17-20, 2018

[5] 민소연, 이재승, IoT 환경에서 안전한 통신을 위한 인증 및 그룹 키 관리 기법, Journal of the Korea Academia-Industrial cooperation Society Vol. 20, No. 12 pp. 76-82, 2019